Office of the Auditor General of Ontario
Bureau de la vérificatrice générale de l'Ontario

Information and Information Technology General Controls

Chapter 4: Toward Better Accountability

Why We Did This Audit

- To gain an understanding of the processes and controls in the critically important area of information and information technology (I&IT) systems.
- To assess whether there are effective general controls in place to maintain the integrity of the government's I&IT systems. This initial assessment will inform our future IT-focused value-for-money audits.

Why It Matters

- The Ontario Government relies on I&IT to deliver a wide variety of services and operations in areas such as health, education, social services and justice.
- I&IT general controls are the first level of defence against threats such as hacking, viruses, sabotage, theft and unauthorized access to information and data.

What We Found

- There was no corporate I&IT strategy in place between 2013 and 2016.
- Service-level agreements are important because they clarify the types and quality of service to be provided, how decisions over I&IT systems will be made, and how performance will be assessed. Yet we found that 75% of government I&IT systems do not have service-level agreements in place.
- Two of the systems we audited, Courts and Licensing, were flagged as overdue for replacement and modernization in 2009/10, but still have not been modernized. An attempt was made at modernizing the Courts system, but it failed and $4.5 million was written off. The Licensing system, initially planned to be modernized by 2016 at an estimated cost of $230 million, has been significantly delayed and is not expected to be finished until 2025.
- Maintenance for the Courts and Licensing systems has been minimal since 2009, and restricted to levels that allow the ministries to meet only their legislative requirements, not to enhance service delivery.
- We noted issues, to varying degrees, with all three I&IT systems, including instances where users were granted inappropriate access to sensitive and confidential data.
- None of the three systems we audited conducted root-cause or trend analyses on incidents to help I&IT clusters to identify and address interrelated and recurring incidents that have a wider impact on I&IT performance.

Conclusions

- I&IT clusters should revisit system modernization timelines and identify areas where these timelines could be moved up. Appropriate strategies should be put in place to ensure the systems are sufficiently maintained to mitigate the deterioration of system performance.
- All three systems need improvement, including implementing controls to establish service-level agreements, prevent unauthorized access to confidential information and effectively manage problems.
- All three systems had adequate processes and controls in place to address the risks arising due to availability and capacity management, business continuity and disaster recovery.

To view the report, please visit www.auditor.on.ca